UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of	)	
IN THE MATTER OF THE SEARCH OF INFORMATION	)	
ASSOCIATED WITH THE GOOGLE ACCOUNT	)	4:24 MJ 9313 RHH
kashdagreat11@gmail.com	)	**FILED UNDER SEAL**
THAT IS STORED AT PREMISES CONTROLLED BY	)	
GOOGLE, LLC	)	SIGNED AND SUMBITTED TO THE COURT FOR
	)	FILING RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Gary Arturo II, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the Northern District of California, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- XX a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section		*Offense Description*
Title	Section	
18	371	Conspiracy
18	2114(a)	Robbery of mail
18	924(c)	Use and carry of a firearm in furtherance of a crime of violence
18	1704	Stealing keys adopted by the Post Office
18	1708	Theft of mail

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ✓ Continued on the attached sheet.
- ❑ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct.

Applicant's signature

Deputy Marshal Gary Arturo II, USMS

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: July 23, 2024

Judge's signature

City and State: St. Louis, Missouri

Honorable Rodney H. Holmes, U.S. Magistrate Judge

Printed name and title

AUSA: Torrie J. Schneider

ATTACHMENT A
4:24 MJ 9313 RHH
Property to Be Searched

This warrant applies to information associated with the Google account **kashdagreat11@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043

ATTACHMENT B
4:24 MJ 9313 RHH
Particular Things to be Seized

I. Items to be disclosed by Google, LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from April 11, 2024 to July 23, 2024, unless otherwise indicated:

a) All business records and subscriber information, in any form kept, relating to the Account, including:

1) Names (including subscriber names, usernames, and screen names);

2) Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3) Telephone numbers (including SMS recovery and alternate sign=-in numbers);

4) Records of session times and durations, and the temporary assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those session, including log-in IP addresses;

5) Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address,

SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;

6) Means and source of payment (including any credit card or bank account number);

7) Change history;

8) The dates and times at which the account and profile were created, and the IP address at the time of sign-up;

9) All Google Drive content;

10) All bookmarks maintained by the account;

11) All services used by the account;

12) All past and current usernames, account passwords, and names associated with the account;

13) All activity logs for the account;

14) All photos and videos uploaded to the account, including in Google Drive and Google Photos, as well as any uploaded photos that have the user tagged in them;

15) All location and maps information, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

16) All Google Voice information;

17) All accounts linked to the account (including linked by creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);

18) For accounts linked by SMS number, information regarding whether the numbers were verified;

19) The content of all emails associated with the account, whether stored in draft form or otherwise associated with the account, including all message content, attachments, and header information; deleted emails;

20) All calendar information;

21) All contact information; and

22) YouTube account data, access IP addresses, third-party app list, third-party app username and password.

b) All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial numbers, Media Access Control (MAC) addresses, International Mobile Identification Numbers (IMEI), Mobile Station Integrated Services Digital Network (MSISDN) telephone facility numbers, International Mobile Subscriber Identity Numbers (IMSI), Subscriber Identity Modules (SIM), Unit Device ID (UDID), Universally Unique Identifiers (UUID), Mobile Equipment Number (MEID), Globally Unique Identifier (GUID), Bluetooth Mac Address, Advertising Identifiers (Ad ID), Ad Set ID, Identifier for Advertisers (IDFA), Google Advertising ID (GAID), FCC ID numbers, Tizen Identifier For Advertising (TIFA), or any other device specific advertising data collection identifier, Global Unique Identifiers (GUID), Integrated Circuit Card Identifier numbers (ICCID), Electronic Serial Numbers (ESN), Serial Number, Mobile Electronic Identity Numbers (MEIN), Mobile Identification Numbers (MIN), Part Number, Product Description, Apple Identifiers, Campaign Identifiers, User Agent strings; Android IDs, and telephone numbers; and

c) Records of user activity for each connection made to or from the Account, including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs.

Google is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

II. Information to be seized by the Government

All information described above in Part I, Section A that will assist in arresting **YAHTIS BAILEY**, who was charged with violations of Conspiracy, in violation of Title 18, United States Code, Section 371; Robbery of Mail, Money, or Other Property of the United States, in violation of Title 18, United States Code, Section 2114(a); Use and Carry of a Firearm During and in Relation to a Crime of Violence, in violation of Title 18, United States Code, Section 924(c); Stealing Keys Adopted by the Post Office, in violation of Title 18, United States Code, Section 1704; and Theft of Mail, in violation of Title 18, United States Code, Section 1708 ("subject offenses"), on April 11, 2024, is the subject of an arrest warrant issued the same day, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4), involving **YAHTIS BAILEY** or the account or identifier listed on Attachment A, relating to the following matters:

a. Evidence of the identity of the creator, user, or person with access or control over the account, including records revealing the whereabouts of such person(s);

b. Evidence of how and when the account was accessed or used, including the chronological and geographic context of account access, use and events relating to the subject offenses and the account subscriber;

c. Evidence of means and source of payment for services, including credit card or bank account numbers or digital money transfer account information;

d. Evidence identifying co-conspirators or aiders and abettors, including records revealing their whereabouts.

e. Evidence identifying the creator or recipient of or establishing the time of creation or receipt of communications, records, or data above.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT kashdagreat11@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, LLC	Case No. 4:24 MJ 9313 RHH **Filed Under Seal** SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Deputy United States Marshal Gary Arturo II**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Deputy United States Marshal with the United States Marshals Service ("USMS") and have been for five years. My current duty assignment is as a Criminal Investigator with the Fugitive Apprehension Strike Force. As part of this assignment I investigate, locate, and apprehend fugitives and support fugitive investigative efforts on behalf of the USMS. As such, I am charged with enforcing all laws in all jurisdictions of the United States, its territories, and possessions. I have both a Master of Arts and a Bachelor of Science in Criminology and Criminal Justice with a minor in Psychology from the University of Missouri-St. Louis. I have completed the Basic Deputy United States Marshals Training Program and the Federal Criminal Investigators Training Program in Glynco, Georgia. During my time with USMS, I have experience utilizing various electronic surveillance measures in several fugitive investigations.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the Google account described herein is being used by **YAHTIS BAILEY** ("**BAILEY**"), who was indicted on April 11, 2024, in the Eastern District of Missouri with Conspiracy, in violation of Title 18, United States Code, Section 371; Robbery of Mail, Money, or Other Property of the United States, in violation of Title 18, United States Code, Section 2114(a); Use and Carry of a Firearm During and in Relation to a Crime of Violence, in violation of Title 18,

United States Code, Section 924(c); Stealing Keys Adopted by the Post Office, in violation of Title 18, United States Code, Section 1704; and Theft of Mail, in violation of Title 18, United States Code, Section 1708 (4:24-CR-170-SEP/JMB) and whose whereabouts are currently unknown. There is also probable cause to believe that the information described in Attachment B will assist law enforcement in arresting **BAILEY**, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On April 11, 2024, a grand jury in the Eastern District of Missouri, indicted **BAILEY** with Conspiracy, in violation of Title 18, United States Code, Section 371; Robbery of Mail, Money, or Other Property of the United States, in violation of Title 18, United States Code, Section 2114(a); Use and Carry of a Firearm During and in Relation to a Crime of Violence, in violation of Title 18, United States Code, Section 924(c); Stealing Keys Adopted by the Post Office, in violation of Title 18, United States Code, Section 1704; and Theft of Mail, in violation of Title 18,

United States Code, Section 1708 (4:24-CR-170-SEP/JMB). Upon receipt of the warrant, the USMS began a fugitive investigation.

7. On July 2, 2024, investigators searched law enforcement databases and discovered that **BAILEY** may be residing with his mother, YOLANDA GREEN ("GREEN") at 11050 Shannon Circle, Hampton, Georgia 30228. GREEN is age appropriate to be **BAILEY**'s mother and has a history of shared addresses with **BAILEY**.

8. Investigators also queried previous booking photographs of **BAILEY** and discovered that he has a "YOLANDA" tattoo on his arm.

9. On July 8, 2024, investigators with the United States Postal Investigation Service provided results of a mail cover for 11050 Shannon Circle, Hampton, Georgia 30228. Two pieces of mail delivered to that address in June 2024 were addressed to **BAILEY**. One appeared to be from a collection agency in Middletown, Ohio and the second was from Capital One Auto Finance based in Plano, Texas.

10. On July 8, 2024, investigators received information from Capital One that **BAILEY** had applied for an auto loan in April 2024, but it was declined. **BAILEY**'s name was on the loan application and the physical address was 11050 Shannon Circle, Hampton, Georgia. The loan application also listed an email address: **kashdagreat11@gmail.com**.

11. Additionally, agents learned that between late June and early August 2023, AT&T toll and usage records associated with BAILEY's phone number listed **kashdagreat11@gmail.com** as an associated email address.

12. In my training and experience, many fugitives avoid traditional telephonic communication with friends and relatives, believing law enforcement can easily track their whereabouts via telephone. A trend by many fugitives is to use web-based applications and communication services to facilitate communication with friends and relatives, while simultaneously limiting their calls and text messages with regular service providers. The types of data that may be stored in a Google account can provide information concerning new or additional cellular devices, Internet Protocol ("IP") addresses, email addresses, location information, downloaded third-party applications, and other information that law enforcement may use to identify **BAILEY's** location.

BACKGROUND CONCERNING GOOGLE[1]

13. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether they have a Google Account, a free web browser called Google Chrome, a free search engine called

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

14. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

15. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

16. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

17. I have learned the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using the Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents*. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Android ID, Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

v. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's websites). Google also retains information regarding accounts registered from the same IP address.

18. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

19. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

20. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to

connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

21. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

22. In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

a. *Google Drive content*. Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs*. Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a

service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive.

c. *Google Photos*. Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or "Exif") data and can include GPS location information for where a photo or video was taken.

d. *Google Calendar*. Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content*. Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's email and chat content.

f. *Location History data*. Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

g. *Google Payments*. Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Google Profile*. Google allows individuals to create a Google profile with certain identifying information, including pictures.

i. *Google Plus*. Google hosts an Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply "friends") into Circles. In addition, Google has a service called PlusOne, in which Google recommends links and posts that may be of interest to the account, based in part on accounts in the user's Circle having previously clicked "+1" next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user's Circle.

j. *Chrome Browser and Search History*. Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at http://www.google.com (and variations thereof, including http://www.google.ru), and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

23. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

24. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under

investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

25. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information to conceal evidence from law enforcement).

26. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. (*e.g.,* if money laundering is involved, a list of apps might reveal banking institutions used by the target) In addition, emails, photos, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

CONCLUSION AND REQUEST FOR SEALING

27. Based on the forgoing, I request that the Court issue the proposed search warrant. Under 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it,

reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

28. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury the foregoing is true and correct.

Respectfully Submitted,

_____

Gary Arturo, II, Deputy U.S. Marshal
United States Marshal Service

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 23rd day of July, 2024.

_____

RODNEY H. HOLMES
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF MISSOURI

ATTACHMENT A
4:24 MJ 9313 RHH
Property to Be Searched

This warrant applies to information associated with the Google account **kashdagreat11@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043

ATTACHMENT B
4:24 MJ 9313 RHH
Particular Things to be Seized

I. Items to be disclosed by Google, LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from April 11, 2024 to July 23, 2024, unless otherwise indicated:

a) All business records and subscriber information, in any form kept, relating to the Account, including:

1) Names (including subscriber names, usernames, and screen names);

2) Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3) Telephone numbers (including SMS recovery and alternate sign=-in numbers);

4) Records of session times and durations, and the temporary assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those session, including log-in IP addresses;

5) Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address,

SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;

6) Means and source of payment (including any credit card or bank account number);

7) Change history;

8) The dates and times at which the account and profile were created, and the IP address at the time of sign-up;

9) All Google Drive content;

10) All bookmarks maintained by the account;

11) All services used by the account;

12) All past and current usernames, account passwords, and names associated with the account;

13) All activity logs for the account;

14) All photos and videos uploaded to the account, including in Google Drive and Google Photos, as well as any uploaded photos that have the user tagged in them;

15) All location and maps information, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

16) All Google Voice information;

17) All accounts linked to the account (including linked by creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);

18) For accounts linked by SMS number, information regarding whether the numbers were verified;

19) The content of all emails associated with the account, whether stored in draft form or otherwise associated with the account, including all message content, attachments, and header information; deleted emails;

20) All calendar information;

21) All contact information; and

22) YouTube account data, access IP addresses, third-party app list, third-party app username and password.

b) All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial numbers, Media Access Control (MAC) addresses, International Mobile Identification Numbers (IMEI), Mobile Station Integrated Services Digital Network (MSISDN) telephone facility numbers, International Mobile Subscriber Identity Numbers (IMSI), Subscriber Identity Modules (SIM), Unit Device ID (UDID), Universally Unique Identifiers (UUID), Mobile Equipment Number (MEID), Globally Unique Identifier (GUID), Bluetooth Mac Address, Advertising Identifiers (Ad ID), Ad Set ID, Identifier for Advertisers (IDFA), Google Advertising ID (GAID), FCC ID numbers, Tizen Identifier For Advertising (TIFA), or any other device specific advertising data collection identifier, Global Unique Identifiers (GUID), Integrated Circuit Card Identifier numbers (ICCID), Electronic Serial Numbers (ESN), Serial Number, Mobile Electronic Identity Numbers (MEIN), Mobile Identification Numbers (MIN), Part Number, Product Description, Apple Identifiers, Campaign Identifiers, User Agent strings; Android IDs, and telephone numbers; and

c) Records of user activity for each connection made to or from the Account, including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs.

Google is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

II. Information to be seized by the Government

All information described above in Part I, Section A that will assist in arresting **YAHTIS BAILEY**, who was charged with violations of Conspiracy, in violation of Title 18, United States Code, Section 371; Robbery of Mail, Money, or Other Property of the United States, in violation of Title 18, United States Code, Section 2114(a); Use and Carry of a Firearm During and in Relation to a Crime of Violence, in violation of Title 18, United States Code, Section 924(c); Stealing Keys Adopted by the Post Office, in violation of Title 18, United States Code, Section 1704; and Theft of Mail, in violation of Title 18, United States Code, Section 1708 ("subject offenses"), on April 11, 2024, is the subject of an arrest warrant issued the same day, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4), involving **YAHTIS BAILEY** or the account or identifier listed on Attachment A, relating to the following matters:

a. Evidence of the identity of the creator, user, or person with access or control over the account, including records revealing the whereabouts of such person(s);

b. Evidence of how and when the account was accessed or used, including the chronological and geographic context of account access, use and events relating to the subject offenses and the account subscriber;

c. Evidence of means and source of payment for services, including credit card or bank account numbers or digital money transfer account information;

d. Evidence identifying co-conspirators or aiders and abettors, including records revealing their whereabouts.

e. Evidence identifying the creator or recipient of or establishing the time of creation or receipt of communications, records, or data above.